CUSTOM APPLICATION BEHAVIOURAL SECURITY MONITORING USING SIEM
AGENDA FOR TODAY

• Introduction
• Problem Statement
• Application Security Monitoring Process
• Q & A
WHO ARE WE?

Himanshu Tonk
Junior Manager, Cyber Risk Services
Deloitte Netherlands
Expertise: Security Monitoring, Threat Hunting

Prithvi Bhat
Junior Manager, Cyber Risk Services
Deloitte Netherlands
Organisations struggle to identify relevant threats and setting up security monitoring/detection.

Alignment of security requirements to business objectives.

Availability of usable data that can be converted into tangible use-cases.

Expertise in building advanced monitoring content.
### Five step Process

<table>
<thead>
<tr>
<th>Identification &amp; Threat Modelling of Critical Application</th>
<th>Onboarding</th>
<th>Implementation</th>
<th>Documentation</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Selection of application for monitoring</td>
<td>• Connecting &amp; ingesting security data in to monitoring platform</td>
<td>• Security content development</td>
<td>• Purpose &amp; design document</td>
<td>• Tuning of the security content based on feedback &amp; knowledge gained</td>
</tr>
<tr>
<td>• Threat modelling to uncover the underlying threats</td>
<td>• Alerting &amp; follow-up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Playbooks</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### IDENTIFICATION AND RATING OF POTENTIAL APPLICATIONS BY SCORING THEM ALONG THREE FACTORS

<table>
<thead>
<tr>
<th>Actual risk coverage</th>
<th>Speed of implementation</th>
<th>Visibility within Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk mitigated, based on the threats, exposure and potential impact.</td>
<td>Ease and speed of onboarding the application and its use-cases.</td>
<td>Ability to show the added business value of security monitoring.</td>
</tr>
</tbody>
</table>
ONBOARDING APPLICATIONS IS DONE USING A STANDARDIZED THREAT MODELING AND USE CASE DESIGN PROCESS

1. Selection of the business processes to be analyzed
   - Input
     • Risk assessment
     • Output of the previous step

2. Determination of the underlying IT infrastructure
   - Input
     Network / architecture maps

3. Execution of an attack path analysis
   - Inputs
     • Red team reports
     • Vulnerability management reports
     • Architecture maps

4. Evaluation of existing cyber security controls

5. Identification of aspired detection controls (use cases)

6. Use case design & building
ONBOARDING OF IDENTIFIED APPLICATION/S TO THE MONITORING PLATFORM

- Read up on technology stack if not yet familiar.
- Retrieve relevant documentation and gain an understanding what is possible within the tech stack.
- Structure received sample logs, categorize available events and gain understanding of types of events available.
- Use previous research to identify and add events not present in sample.
- Deep-dive into log sources to identify events that are relevant to the identified use-cases.
- Make initial estimate of performance impact on SIEM and the application itself.
- Make initial estimate whether tuning the amount of alerts to acceptable and usable levels is possible.
- Define path to the monitoring platform and organize access.
- Test run data connections and connect data to the platform in the final form.
IMPLEMENTATION OF DESIGNED USE-CASES IN MONITORING PLATFORM

Building Security Use-Cases
- Development of logical statement for detection
- Assign the actions to execute once triggered

Testing
- Test the logic against data
- Monitor the performance of use-cases

Deploy in Production
- Setup the use-cases in production to alert
DOCUMENTATION

Purpose & Design Statement
- Goal of the use-case and monitored threat
- Technical design of the use-case

Playbooks
- Investigation steps to triage the alert
- Should include relevant stakeholders and type of notification
MAINTENANCE OF USE-CASES

Identify
• Identify the tuning opportunity

Implement
• Modify the logic to whitelist/blacklist the activity.

Document
• Document the changes performed for knowledge purpose

Regular tuning is the key to effective use-cases
CONCLUSIONS

1. Sneak peak in to threat of organization

2. Security monitoring implementation becomes a quick win following this systematic approach

3. Reusable process which appears to be complex at first seems simple after first iteration.

4. Focused and prioritized detection
Please don't ask tough questions